局域网环境下安全准入认证方法的研究

Security authentication access control in LAN environment

贾亚军　刘 磊　杨 敏　关 宇
（新疆油田公司勘探开发研究院地球物理研究所　新疆乌鲁木齐 830013）

摘要：在局域网环境中，只要存在物理的连接端口，未经授权的网络设备或用户就可能通过连接到局域网的网络设备自动的进入网络，造成极大的安全隐患。同时，基于端口的 VLAN 分配缺乏灵活性、不可控的 IP 存取易造成 IP 地址冲突等网管问题。这些问题的有效解决，在企业局域网环境中，已显得十分重要。我们通过研究近年来大型局域网身份和授权技术并将其实施在企业局域网中，有效解决上述问题。

关键词： RADIUS　认证、授权、记帐（AAA）　EAP　IEEE 802.1x　基于用户的 VLAN

1　引言

企业计算机网络网络安全采取的总体策略应该是分层设计、纵深防御。本文意在通过对大型企业局域网环境下身份认证与授权技术的分析、试验及实施，建立在网络端口上认证和存取控制，从而完善网络安全，降低由企业内部造成的网络安全隐患。

我们总结通常企业局域网常见的弊端如下：

（1）不设防的非认证网络存取。基于以太的局域网环境不提供用户和网络设备的认证。这是由 TCP/IP over Ethernet 的机制所决定的。即 ARP 和 DHCP 不提供用户的认证/授权/记帐，只提供网络的互连。这就造成在局域网环境中，只要存在物理的连接端口，未经授权的网络设备或用户就可能通过连接到局域网的设备自动的进入网络，造成极大的安全隐患。对于那些与外界交往密切、外来人员可从员工办公室直接接入到企业局域网的企业、潜在的危害就更大。

（2）IP 地址冲突。无论网管用不用 DHCP，都易造成企业局域网的 IP 地址冲突。如用 DHCP 时，如果某个用户不遵守规则，同样会造成 IP 地址冲突。

（3）基于端口的 VLAN 分配缺乏灵活性。同基于用户的 VLAN 分配相比较，这一点显而易见。

以上这些问题的解决，在企业局域网环境中，已显得十分重要。通过研究最新的局域网安全准入机制及适合于企业局域网的管理办法，解决上述问题。

2　可供采用的关键新技术

2.1　Remote Authentication Dial－In User Service（RADIUS）

RADIUS 在早期主要应用于远程存取路由器上，一个典型应用的例子就是 Cisco 的远程拨号访问的 AAA 控制。现在交换机已经开始支持 RADIUS 协议，这就意味着以太局域网环境现在可以享受到存取控制方案带来的好处。一个明显的例子就是：现在可以通过 RADIUS 协议，部署基于用户的 VLAN。我们在分析 Cisco Catalyst 交换机（作为访问存取或分布层设备）时，注意到在新的 IOS 版本支持下，这些交换机已经开始支持 RADIUS VLAN ID 的分配。

2.2　Extensible Authentication Protocol（EAP）

EAP 是由 IETFRFC 2284 和 IEEE 802.1x 标准所定义的协议。这使得在以太局域网环境中部署 RADIUS 协议成为可能。802.1x 标准，也称 EAP over LAN（EAPoL），将 EAP 的应用扩展到了具有广播介质功能的网络，EAPoL 通过交换机在最终用户和 AAA 服务器之间提供了一个通信通道。有了 AAA 支持的用户访问存取控制，由最终用户发起的的所有以太局域网的连接请求都可以被认证，但只有那些具有有效信任关系的以太局域网的连接请求才被许可。

2.3　基于用户的授权机制

用户在获取到 RADIUS 许可的同时得到已定义的用户授权，包括 DHCP 分配的 IP 地址及动态 VLAN 属

性。用户不能更改客户端的网络配置，彻底解决局域网环境中 IP 地址冲突的问题。

3 IEEE 802.1x 协议的体系结构

IEEE 802.1x 协议的体系结构包括三个重要的部分：Supplicant System 客户端、Authenticator System 认证系统、Authentication Server System 认证服务器。图1描述了三者之间的关系以及互相之间的通信。

客户端系统一般为一个用户终端系统。通常要安装一个客户端软件，用户通过启动这个客户端软件发起 802.1x 协议的认证过程。为支持基于端口的接入控制，客户端系统需支持 EAPOL（Extensible Authentication Protocol Over LAN）协议。

图中认证系统的受控端口处于未认证状态，因此无法访问认证系统提供的服务。认证系统的 PAE 通过不受控端口与 Supplicant PAE 进行通信，二者之间运行 EAPOL 协议。认证系统的 PAE 与认证服务器之间运行 EAP（Extensible Authentication Protocol）协议。

认证系统和认证服务器之间的通信可以通过网络进行，也可以使用其他的通信通道。如果认证系统和认证服务器集成在一起，二个实体之间的通信就可以不采用 EAP 协议。

认证服务器通常为 RADIUS 服务器，该服务器可以存储有关用户的信息，比如用户所属的 VLAN、CAR 参数、优先级、用户的访问控制列表等。当用户通过认证后，认证服务器会把用户的相关信息传递给认证系统，

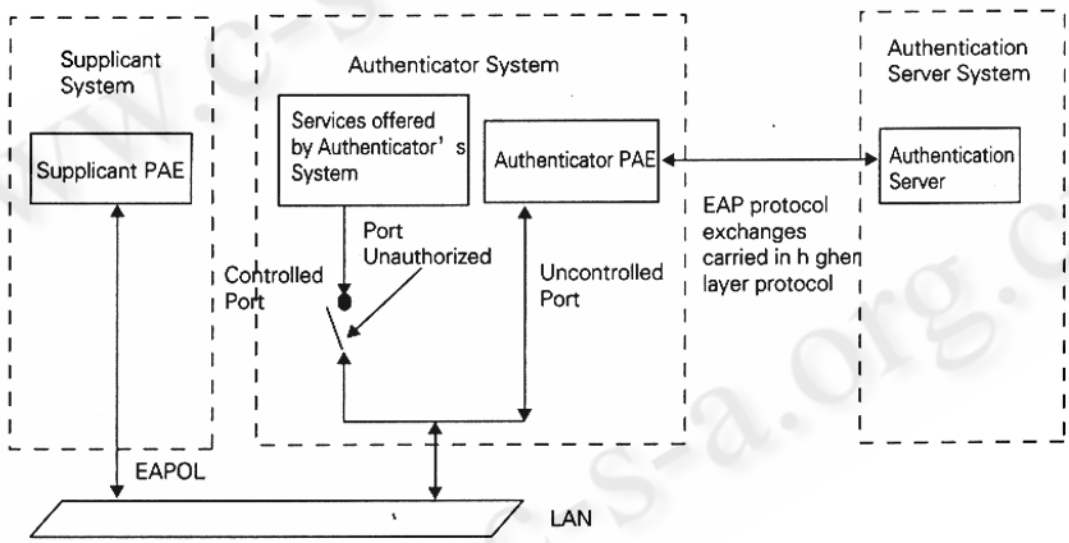

图 1

认证系统通常为支持 802.1x 协议的网络设备。该设备对应于不同用户的端口（可以是物理端口，也可以是用户设备的 MAC 地址）有两个逻辑端口：受控（controlled Port）端口和不受控端口（uncontrolled Port）。不受控端口始终处于双向连通状态，主要用来传递 EAPOL 协议帧，可保证客户端始终可以发出或接受认证。受控端口只有在认证通过的状态下才打开，用于传递网络资源和服务。受控端口可配置为双向受控、仅输入受控两种方式，以适应不同的应用环境。如果用户未通过认证，则受控端口处于未认证状态，则用户无法访问认证系统提供的服务。

由认证系统构建动态的访问控制列表，用户的后续流量就将接受上述参数的监管。认证服务器和 RADIUS 服务器之间通过 EAP 协议进行通信。

4 整体解决方案

经过对多个局域网安全准入认证的解决方案的分析及测试，我们认为在以太局域网环境中，网络设备和最终用户端的操作系统对 RADIUS/IEEE 802.1x 标准构架的应用尚处在起步阶段。一个最新的变化就是本文前面提到的 Cisco Catalyst 2950 和 3550 交换机（作为访问存取或分布层设备）在新的 IOS 版本下已经开始

支持 RADIUS VLAN ID 的分配。这就意味着如果采用这种技术，除了能完成安全准入认证的功能，还能真正实现基于用户 VLAN 的划分。过去，这种技术的实现是比较复杂的，并且是难以实现的。采用了这种局域网安全准入认证技术，不但能减少技术的投资，而且它能和其他的网络技术，例如：DHCP、DNS、LDAP 甚至 CA/PKI 相结合，从而形成包含网络安全准入认证/网络管理的整体解决架构，为网络、数据库应用及系统等提供了行之有效的安全机制。另外，可以大大减轻网络管理人员的负担。

802.1x 标准构架为基础，结合 Cisco ACS 的 AAA 机制及动态 DNS/DHCP、企业级 CA 中心/LDAP 的全面局域网安全准入认证的解决方案实施于企业局域网局域网环境中。

4.1 实验环境的建立

在企业局域网环境中搭建如图 2 的实验环境：

Workstation Clients 采用 WindowsXP 连网客户机，已知的操作系统的支持状况见表 1。

Cisco Catalyst 2950 / Catalyst 3550/ 指 IOS 为 Version 12.1(14)EA1a，作为网络的访问接入层交换机。

Table 2-1 Comparison of Widely Available 802.1x/EAP Authentication Protocols

	802.1x/EAP Compliance	Mutual Authentication	Dynamic Wired Equivalent Privacy Support	Operating System Support
Cisco EAP (LEAP)	Yes	Yes	Yes	Windows platforms (Windows XP, 2000, 98, 95, ME and NT), Windows CE, Linux, Disk Operation System (DOS), and Mac OS
EAP-TLS	Yes	Yes	Yes	Windows XP[1]
EAP MD5	Yes	No	No	Windows XP[1]

1. Note: Microsoft has announced EAP support for legacy operating systems in 2002 (Windows 2000, Windows NT 4, Windows 98, Windows 98 Second Edition, and Windows ME). Also, there are third-party EAP supplicants that provide support for EAP-TLS on various operating systems (Meetinghouse Data Communications EAP supplicant, for example).

表 1

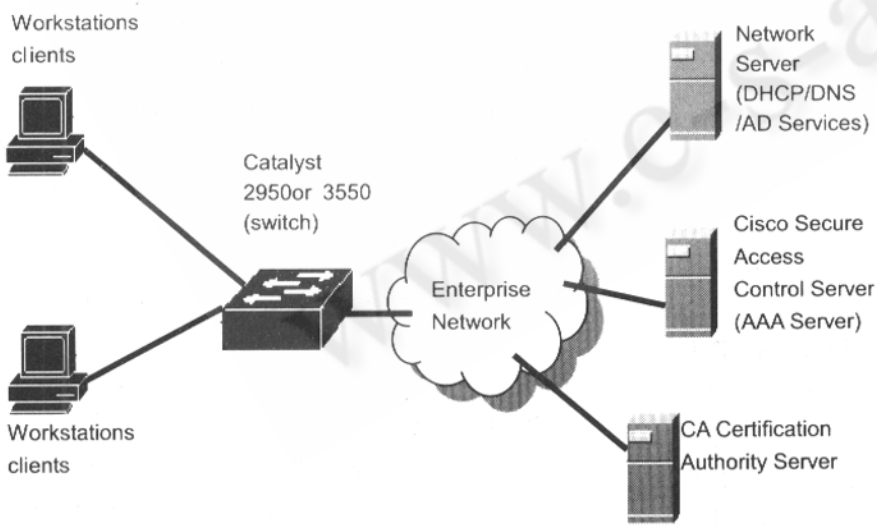

图 2

Cisco Catalyst 6509 指 IOS 为 Version 12.2(17a)SX1 作为网络的核心交换机，不但支持 RADIUS/IEEE 802.1x 标准构架，还支持 RADIUS VLAN ID 的分配。

Cisco Secure Access Control Server（AAA Server）指 Cisco Secure ACS 3.2 for Windows。它是 RADIUS 服务器。

Network Server（DHCP/DNS / AD（Microsoft）Services）是网络管理和网络应用的服务器。AD 服务器作为 AAA Server 的后台用户数

（下转第 103 页）

综上所述、我们最终选择了以采用 RADIUS/IEEE

(上接第 99 页)

据库,采用 PEAP(EAP－MSCHAPv2)协议。

CA(Certification Authority)指启用 AD Server 的 CA 服务,作为局域网环境中的证书服务器、管理客户机和 Cisco ACS 的证书。

4.2 实验环境中的主要测试内容

(1) 使用基于 802.1x 的用户身份认证/启用 802.1x PEAP 加密机制。

(2) 实现动态 ACS 划分 Vlan。

(3) 实现 ACS 和 Win2K 的数据库同步及用户三级身份认证。

(4) 使用 DHCP 动态分配 IP 地址。

(5) 实现 ACS、DHCP、AD、NAS、CA 的协同工作。

(6) 用户重新认证的实现。

5 结论

我们在搭建的局域网环境中全面完成了预期测试内容,符合设计需求。其整体解决方案在局域网环境中是完全可行的。以 Cisco ACS 为 3A 认证的网络安全机制提高了企业局域网在网络安全及信息安全方面的"保险系数"。它的主要目的在于进一步加强网络安全、实现局域网环境下用户的认证、授权及记帐,对网络环境的各种信息应用具有较强的实用功能。

参考文献

1 User Guide for Cisco Secure ACS for Windows Server Version 3.2.

2 Installation Guide for Cisco Secure ACS for Windows Server Version 3.2.